**Commission of Inquiry**
**into the Actions of Canadian Officials in Relation to Maher Arar**
**Policy Review**

# Accountability of Security Intelligence in Canada
# A Background Paper
# to the Commission's
# Consultation Paper

**December 10, 2004**

106-03479/

## TABLE OF CONTENTS


A. THE PRE-HISTORY OF NATIONAL SECURITY ACCOUNTABILITY TO 1984 ..... 1
B. THE McDONALD COMMISSION AND ACCOUNTABILITY ..... 5
C. ACCOUNTABILITY INNOVATIONS IN THE *CSIS ACT* ..... 8
1. The statutory mandate ..... 10
2. Ministerial control and responsibility ..... 12
(i) Office of the Inspector General ..... 13
3. Judicial control ..... 14
4. Independent review: SIRC ..... 16
D. THE SECURITY INTELLIGENCE REVIEW COMMITTEE ..... 16
1. Membership ..... 16
2. Overview: SIRC Mandate ..... 17
(i) Targeting ..... 21
(ii) Foreign Intelligence ..... 23
(iii) Foreign Arrangements ..... 24
(iv) Warrants ..... 25
(v) Complaints ..... 27
3. Reporting by SIRC ..... 31
4. SIRC and CSIS: two decades of evolution in the review process ..... 32
(i) 1984-1989/90: ..... 32
(ii) 1990-2001: ..... 33
(iii) 2001-present: ..... 34
E. THE CSE COMMISSIONER ..... 35
1. Introduction ..... 35
2. History of CSE Review Proposals ..... 37
3. Establishment of CSE Commissioner ..... 39
4. Current Mandate of the CSE Commissioner ..... 41
(i) Review Duties ..... 42
(ii) Complaints Duties ..... 43
(iii) "Public Interest Defence" Duties ..... 44
F. THE AUDITOR GENERAL ..... 44
G. THE INFORMATION AND PRIVACY COMMISSIONERS ..... 46
H. PARLIAMENTARY REVIEW ..... 49

## A. THE PRE-HISTORY OF NATIONAL SECURITY ACCOUNTABILITY TO 1984

National security has long been a cause for concern for Canadians. Are governments doing enough to protect Canadians from threats to security and maintain public safety? Are the rights and liberties of Canadians threatened by the exercise of national security powers? These are questions that, in various forms, have echoed down the decades.

During World War II, there was alarm about enemy 'fifth columnists' undermining the war effort at home. Many who were believed to pose potential threats to the security of Canada were interned, organizations banned, and censorship imposed. Although broadly supported by Parliament and public opinion at the time, doubts about the government's actions later grew. The most notorious case was that of the Japanese Canadian population of the West Coast, more than 20,000 of whom were forcibly removed to camps in the interior as alleged, but never proven, threats to security in a war against Japan. In 1988, the government of Canada offered a formal apology and financial compensation to the Japanese Canadian community for the wartime wrongs done to them.

In 1945-6, a cipher clerk in the Ottawa embassy of the Soviet Union, Igor Gouzenko, defected to Canada with documentary evidence of an extensive Soviet spy ring operating in Canada. Gouzenko's revelations helped ignite the Cold War, yet the way in which the government of Canada handled this explosive issue left many unanswered questions. A secret order in council under the *War Measures Act* authorized the detention and interrogation of a number of suspects, without benefit of legal counsel. A royal commission took secret evidence and then published a report in which some two dozen persons were named as betraying their country on behalf of a hostile foreign power, even though only about half of those named were ever subsequently convicted of espionage or related offences in a court of law[1]. In the aftermath of the Gouzenko affair, following the recommendations of the royal commission, the government of Canada

---

[1] Report of the Royal Commission appointed to investigate the facts relating to and the circumstances surrounding the communication, by public officials and other persons in positions of trust of secret and confidential information to agents of a foreign power, Hon. Mr. Justice Taschereau and Hon. Mr. Justice R.L. Kellock, Commissioners, 27 June 1946.

constructed a peacetime national security state, with security screening of public servants, and later of immigrants and citizenship applicants, and an extensive domestic surveillance operation by the RCMP Security Service.

Despite these developments, and despite public notice of issues around national security, at first there was little attention paid to the question of the accountability of the agencies engaged in national security. By and large, Canadians seemed content to let national security agencies do their work in secret, unchecked by any external scrutiny of the efficacy or propriety of their operations. Part of the explanation may lie in the relatively consensual and bipartisan nature of debates over national security during the war and the early Cold War years.

It was only in the 1960s, in the second decade of the Cold War, that the first serious stirrings of concern about a lack of accountability were raised. In 1965, two security-related scandals erupted, quickly becoming partisan political issues. The firing of a Vancouver postal worker as a suspected Soviet spy caused a public outcry. Then the 'Gerda Munsinger' affair implicated two Cabinet ministers in the previous Progressive Conservative government in a relationship with a woman believed to have connections to Soviet espionage. Under considerable pressure from Parliament and the press, Prime Minister Lester Pearson called two separate commissions of inquiry into these affairs, and then followed these up with a wider royal commission on security, known as the Mackenzie Commission. The terms of reference for this latter inquiry were to "examine the operations of the Canada's security procedures with a view to ascertaining, firstly, whether they were adequate for the protection of the state against subversive action and, secondly, whether they sufficiently protect the rights of private individuals in any investigations which are made under existing procedures."[2]

The Mackenzie Commission reported in 1969[3] and made the first official recommendation for a formal accountability mechanism for the Security Service – a Security Review Board nominated

---

[2] House of Commons, Debates, March 7, 1966, v. III, p. 2297.

[3] Commission of Inquiry into complaints made by George Victor Spencer, The Hon. Me Justice Dalton Wells, Commissioner, July 1966; Commission of Inquiry into matters relating to one Gerda Munsinger, The Hon. Mr Justice Wishart Spence, Commissioner, September 1966; *Report of the Royal Commission on Security* (Abridged), June 1969.

by the Governor in Council, but "independent of any government department or agency".[4] The Board's main job would be to hear appeals from public servants, immigrants, and citizenship applicants denied security clearance. The Board would also receive periodic reports from the head of the Security Service and would have "authority to draw to the attention of the Prime Minister any matter it considers appropriate,"[5] a clear indication of executive accountability, but with no reference to parliamentary or other forms of accountability. This recommendation was linked to another recommendation, that the Security Service be detached from the RCMP and reformed as a "new civilian non-police agency...quite separate from the RCMP...without law enforcement powers".[6] The status of the Security Service as a branch of a police force was seen as an obstacle to developing accountability, in part due to concerns regarding "police independence". The Mackenzie Commission tried to avoid this problem by linking 'civilianization' of the Security Service with an accountability mechanism for a new body with no law enforcement powers. Neither recommendation was implemented at the time.

A change in the organization of government in 1965-66 was to have considerable future importance for the development of national security accountability, although the significance was not fully appreciated at the time.[7] A new ministry, that of the Solicitor General, was created, including, among other responsibilities, the RCMP.[8] Until this time, the RCMP had been the responsibility of the Minister of Justice and Attorney General. The latter office is responsible for initiating criminal prosecutions and, in this capacity, is traditionally expected to maintain an arm's-length relationship with the Cabinet. Placing the RCMP administratively under the new office of Solicitor General provided for the first time a potential line of ministerial responsibility for the Security Service, although this took some time to develop fully in practice. Indeed, it had to await the separation of the Security Service from the RCMP some twenty years later.

---

[4] *Report of the Royal Commission on Security*, para. 299, p. 109.

[5] *Ibid.*, para. 199 (d), p. 110.

[6] *Ibid.*, para. 297, p. 105.

[7] J. Ll. J. Edwards, *Ministerial Responsibility for National Security*, study prepared for the Commission of Inquiry Concerning Certain Activities of the RCMP (Ottawa: Supply & Services Canada, 1980) pp. 21-40.

[8] Order in Council PC 1965 – 2286, 22 December 1965; 14-15 Eliz. II, c. 25, s. 4.

Following the Mackenzie Commission in 1969, the political context for national security issues changed significantly. Throughout the 1960s, the Security Service had been directing attention to the emergent Quebec sovereignty movement, especially the violent terrorist wing that had begun some forms of armed struggle against the Quebec and Canadian governments. In October 1970, cells of the Front de libération du Québec (FLQ) kidnapped the British trade commissioner, James Cross, and kidnapped and later murdered the Quebec minister of labour, Pierre Laporte. The Canadian government, acting upon the request of the Quebec government, invoked the *War Measures Act* on the basis of an 'apprehended insurrection', suspending normal civil liberties, detaining a number of individuals without charge and without legal counsel, applying censorship of the press, and declaring certain organizations retroactively illegal.

Following the resolution of this crisis, the federal government, in conjunction with the Quebec and Montreal police, stepped up intrusive surveillance of the separatist movement in Quebec, employing countering methods that in some cases were of doubtful legality, including break-ins, mail openings, property destruction, intimidation of individuals, and what were widely termed 'dirty tricks' by the police. When some of these methods came to light in the media during the 1970s, questions arose around national security and the specific role of the RCMP Security Service in illegal acts. Intrusive methods were now seen to be used not just against small groups allied to a hostile foreign power – as was widely believed to be the case for the Canadian Communist party (linked to the USSR) that was targeted by the security service throughout the Cold War – but against domestic political forces, an inherently more controversial matter.[9]

By 1976, the sovereigntist Parti Québécois (PQ) had come to office in Quebec, and launched its own inquiry into police activities.[10] It was unclear to what extent the federal government, via its Security Service, distinguished between threats to national security, clearly posed by the terrorist wing of the sovereignty movement, and threats to national unity posed by the democratic and

---

[9] Journalistic accounts of the public scandals surrounding the RCMP include John Sawatsky, *Men in the Shadows: the RCMP Security Service* (Toronto: Doubleday, 1980); Jeff Sallot, *Nobody Said No* (Toronto: Lorimer, 1979). See also Reg Whitaker, 'Canada: the RCMP scandals', in Andrei S. Markovits and Mark Silverstein, eds., *The Politics of Scandal: Power and Process in Liberal Democracies* (New York: Holmes & Meier, 1988) pp. 38-61.

[10] Jean Keable et al, *Rapport de la Commission d'enquête sur les opérations policières en territoire québécois* (Government of Quebec, Ministry of Justice, 1981).

strictly law-abiding PQ. If the latter proved to be a target of extra-legal surveillance methods, this raised serious issues about liberal democracy of much wider concern to Canadians than to Quebec sovereignists alone. These developments gave rise to increasingly vocal demands for greater accountability and transparency in the operations of the federal Security Service. In 1977, the McDonald Commission was appointed to inquire into "certain activities of the RCMP".[11]

## B. THE McDONALD COMMISSION AND ACCOUNTABILITY

The McDonald Commission recommended in 1981 a relatively complex institutional architecture to achieve an unprecedented degree of accountability over the Security Service, both as internal control and as independent review. One of the key recommendations was the separation of the Security Service from the RCMP and its reconstitution as a civilian agency without law enforcement powers. In the changed political context of the time, McDonald's civilianization proposal, unlike Mackenzie's earlier recommendation[12] was accomplished with the passage of the *Canadian Security Intelligence Service Act*[13] in 1984. While the *CSIS Act* mandated a number of new accountability mechanisms, its provisions were not in all cases similar to McDonald's recommendations. We might first examine McDonald's accountability philosophy and the specific recommendations that flowed from this, in order to assess the actual forms that followed the enactment of the *CSIS Act*.

McDonald began with a clear distinction between accountability as control and accountability as explanation, the former taking the form of internal governmental mechanisms of direction, and the latter taking the form of external and independent review. Both were to be grounded in

---

[11] Order in Council PC 1977-1911, 6 July 1977.

[12] On the political and bureaucratic background to civilianization see James Littleton, *Target Nation: Canada and the Western Intelligence Network* (Toronto: Lester & Orpen Dennys, 1986) pp. 135-62; Reg Whitaker, 'The politics of security intelligence policy-making in Canada 1 1970-84', *Intelligence & National Security* 6:4 (October 1991) pp. 659-65.

[13] R.S.C. 1985, c. C-23 ("*CSIS Act*").

statutory forms that would express the will of Parliament. The major elements of accountability were as follows:[14]

***Internal controls***

*Ministerial*

- General policy as to security methods and priorities should be the responsibility of the Cabinet.

- Co-ordination of security and intelligence activities should be the joint responsibility of the Cabinet, the Privy Council Office, and interdepartmental committees.

- The Prime Minister retains "special" responsibilities in the area, including chairing the Cabinet Committee on Security and Intelligence, and being consulted on all security issues of "major importance".

- The Solicitor General should continue to be the minister responsible for the Security Service, and should take the lead in all policy and legislative matters.

*Administrative*

- The Deputy Solicitor General should be the Minister's deputy in respect to all aspects of direction and control of the agency, and should be prepared to give the Minister informed advice on all aspects of the agency's activities.

- The Cabinet Secretary and Privy Council staff should assist the Prime Minister and Cabinet in discharging their responsibilities.

- Accountability must be ensured by an effective system of communications, within the agency and between the agency and the Deputy Solicitor "to ensure that the

---

[14] Commission of Inquiry Concerning Certain Activities of the RCMP, 2nd report – vol. 2, *Freedom and Security Under the Law* (Ottawa: Supply & Services Canada, August 1981) pp. 842-3.

Minister is informed of all those activities which raise questions of legality or propriety."

*Financial*

- An effective system of financial control should be maintained by the Treasury Board, and the Auditor General.

***External review***

*Parliamentary*

- A joint parliamentary committee on security and intelligence should be able to examine the activities of the agency in camera.

*Independent*

- An Advisory Council on Security and Intelligence should be established to assist the Minister, Cabinet, and Parliament in "assessing the legality, propriety, and effectiveness" of the agency. It should be made up of "capable people who will command the respect of Parliament and the public." Lacking executive powers, it should have an "investigating capacity", and should report its findings to the Minister, and as well submit annual reports to the Parliamentary committee.

- A Security Appeals Tribunal should consider appeals regarding security clearance decisions in the areas of public service employment, immigration, and citizenship, and its recommendations made to Cabinet.

*Judicial*

- The use of intrusive surveillance techniques by methods not ordinarily available under law must be submitted to a judge of the Federal Court for approval in specific cases.

- Evidence of illegal activity by members of the agency or their agents must be submitted to the Attorney General to determine whether prosecution should be undertaken.

*Federal/provincial*

- The federal minister and responsible officials should meet regularly with their provincial counterparts to "ensure mutual understanding and co-operation."

*Public*

- Ministers and parliamentarians with responsibilities for security and intelligence should "endeavour to provide the public with all information possible about the security of Canada, the threats to it and steps taken to counter those threats." "A more informed" public can address with better understanding the major issues in the area.

## C. ACCOUNTABILITY INNOVATIONS IN THE *CSIS ACT*

On the road from the Commission recommendations to legislative form in the *CSIS Act*, some changes and new byways were added, and some recommendations dropped altogether.[15]

- With regard to internal controls, the ministerial and administrative lines of responsibility were largely followed, but an additional office, that of the Inspector General, was provided.

- Judicial control over intrusive surveillance methods was adopted in the Act.

- The two proposed independent external review bodies were merged into one body, the Security Intelligence Review Committee (SIRC), an institution exhibiting some significant differences from the models proposed by McDonald. Financial review by the Auditor General was not enshrined in legislation, but was followed up in practice some years later.

---

[15] Stuart Farson, 'Restructuring control in Canada: the McDonald Commission of Inquiry and its legacy', in Glenn P. Hastedt, ed., *Controlling Intelligence* (London: Frank Cass & Co., 1991) pp. 157-188.

- The recommendations regarding federal-provincial co-operation and public information were more hortatory than institutional in nature, being left to political and administrative discretion, although there are specific provisions in the *CSIS Act* referring to co-operative arrangements with the provinces, and provincial police forces, on specific matters.[16]

- The most significant difference was the decision not to follow up on the recommendation regarding a joint parliamentary committee to examine security and intelligence issues *in camera*. There was a provision for a five-year parliamentary review of the Act, as well as an indication that the mandated annual report of SIRC should be tabled in both houses of Parliament after the Minister has first examined it. Apart from these two exceptions, the legislation remains silent on the role of Parliament.

In reaching final legislative form, the *CSIS Act* received wide publicity and was attended by considerable debate. The first draft of the proposed law was met with much criticism, not only from various groups in Canadian society, but also from all the provincial Attorneys General. An unusual procedure was followed in which the Senate considered the draft legislation in committee, recommending significant revisions, which were then largely accepted by the government in the final version of the Act, which drew much less criticism than the original draft. The Senate Committee laid special stress on the differences between security intelligence and law enforcement, and on the "severe consequences on a person's life" that security investigations could have:

> Thus the question of control and accountability becomes important, because there is no impartial adjudication by a third party of the appropriateness of an investigation. Since it is so open-ended and confidential in nature, security intelligence work requires a close and thorough system of control, direction and

---

[16] *CSIS Act*, *supra* note 13, ss. 13(2), 17.

> review, in which political responsibility plays a large part. Such close direction is incompatible with our traditional notions of law enforcement.[17]

Thus the key to understanding accountability in the *CSIS Act* lay in the separation of the Security Service from the RCMP with its law enforcement role. Parliament, the Senate Committee, and the McDonald Commission before them, all proceeded on the basis that accountability, *both as control and as review (explanation)*, was incompatible with the principle of police independence and an arm's length relationship between the executive and law enforcement. The elements of accountability in the *CSIS Act* are discussed below.

**1. The statutory mandate**

The McDonald Commission had been extremely critical of the absence of a legislative mandate of the Security Service when it was located within the RCMP. Following the McDonald Report, the *CSIS Act* itself was to be the bedrock element of accountability for the new agency, laying out in statutory form the fundamental mandate of the agency, its specific powers as well as its limits, and the precise institutional framework in which it was to operate and report.

CSIS is empowered to collect, analyse, and retain information and intelligence "respecting activities that may on reasonable grounds be suspected of constituting threats to the security of Canada" and provide threat assessments to the Government of Canada, or by approved arrangement, to the provinces or to foreign governments or international organizations.[18] Threats to the security of Canada are defined in s. 2, as follows:

> (a) espionage or sabotage that is against Canada or is detrimental to the interests of Canada or activities directed toward or in support of such espionage or sabotage,

---

[17] Report of the Special Committee of the Senate on the Canadian Security Intelligence Service, *Delicate Balance: a Security Intelligence Service in a Democratic Society* (November 1983), p. 6.

[18] *CSIS Act*, *supra* note 13, ss. 12, 13.

(b) foreign influenced activities within or relating to Canada that are detrimental to the interests of Canada and are clandestine or deceptive or involve a threat to any person,

(c) activities within or relating to Canada directed toward or in support of the threat or use of acts of serious violence against persons or property for the purpose of achieving a political, religious, or ideological objective within Canada or a foreign state[19], and

(d) activities directed toward undermining by covert unlawful acts, or directed toward or intended ultimately to lead to the destruction or overthrow by violence of, the constitutionally established system of government in Canada,

but does not include lawful advocacy, protest or dissent, unless carried on in conjunction with any of the activities referred to in paragraphs (a) to (d).

CSIS is thus provided with a relatively precise description of activities it may legitimately target, and those it may not. Espionage, sabotage, terrorism or other forms of political violence, and clandestine foreign-influenced activities detrimental to Canadian interests, are all relatively non-controversial as threats to security.

The inclusion of activities described in 2(d) – in effect, the controversial concept of 'subversive' activities – have led to demands that this definition be removed or modified, especially after 1987, when the Solicitor General directed that the Counter-subversion Branch of CSIS be disbanded, with retained files distributed to more appropriate operational branches.[20] According to critics, the line between activities described in 2(d) and "lawful advocacy, protest or dissent" might not always be easy to draw in practice. It is clear, however, that the definitions of legitimate and illegitimate targets have had important consequences for the accountability of

---

[19] Subsection 2(c) was amended by the *Anti-Terrorist Act* in 2001 to add the words "religious or ideological"; see S.C. 2001, c. 41, s. 89.

[20] See for instance, SIRC, *Amending the CSIS Act, op. cit.*, p. 1.

CSIS, providing a legal baseline for judging the appropriateness of the agency's targeting. Drawing on the definitions of threats to security in the *CSIS Act*, the agency now states that it does not target threats to national unity, such as the lawful forms of the Quebec sovereignty movement, unless they have reason to believe they are being carried out in conjunction with activities described in ss. 2(a) to (d).

## 2. Ministerial control and responsibility

One of the most significant problems identified by the McDonald Commission was the lack of clear ministerial responsibility for the activities of the Security Service. Ministers of the Crown had indicated repeatedly that the principle of police independence compelled them to remain in ignorance of Security Service operations. The best-known iteration of this argument came from then Prime Minister Pierre Trudeau in 1977[21]:

> I have attempted to make it quite clear that the policy of this government, and I believe the previous governments in this country, has been that they…should be kept in ignorance of the day to day operations of the police force and even of the security force. I repeat that this is not a view that is held by all democracies but it is our view and it is one we stand by. Therefore in this particular case it is not a matter of pleading ignorance as an excuse. It is a matter of stating as a principle that the particular minister of the day should not have a right to know what the police are doing constantly in their investigative practices, what they are looking at, and what they are looking for, and the way in which they are doing it….That is our position. It is not one of pleading ignorance to defend the government. It is one of keeping the government's nose out of the operations of the police at whatever level of government.

The *CSIS Act* was designed to fix clear responsibility for CSIS with the Solicitor General.[22] The Director of CSIS is responsible for the control and management of the Service, but "under the

---

[21] Transcript of the Prime Minister's press conference, December 9, 1977. Quoted in Edwards, *Ministerial Responsibility*, *op. cit.*, p. 94.

[22] With a major reorganization of government security functions in early 2004, the Solicitor General has been superceded by the Minister for Public Safety and Emergency Preparedness Canada.

direction of the minister" through the Deputy Minister. Ministerial directives may set "general operational policies" and any other matters on which the Director may be required to consult.[23]

Ministerial control over CSIS is further strengthened by the office of the Inspector General, which is discussed below.

### *(i) Office of the Inspector General*

The Office of the Inspector General (IG) is an innovation which was not part of the McDonald Commission's recommendations. The IG is appointed by the Governor in Council and is responsible to the Deputy Solicitor General. The IG monitors compliance by CSIS with its operational policies, reviews operational activities, and is to have unimpeded access to any information under control of CSIS that the IG deems necessary for the discharge of his or her responsibilities – with the sole exception of 'Cabinet confidences' that may be withheld. The IG submits to the Minister certificates pursuant to periodic reports on the operational activities of CSIS prepared by the Director for the Minister. These certificates attest to the extent to which the IG "is satisfied with the Director's report" and whether in his or her opinion, CSIS activities are in compliance with the Act and with ministerial directives. The certificates also state the IG's opinion as to whether there was any "unreasonable or unnecessary exercise by the Service of any of its powers".[24] These reports and certificates are transmitted to SIRC, but there is no provision for their tabling in Parliament or any form of publication, although parts have from time to time been declassified in redacted form in response to Access to Information requests. In effect, the office of the IG is strictly conceived as a form of internal executive control, with the IG serving as the eyes and ears of the Minister with regard to the activities of CSIS.[25] (The IG may also be

---

[23] *CSIS Act*, ss. 6, 7.

[24] *CSIS Act*, ss. 30-33.

[25] 1996 Report of the Auditor General of Canada, s. 27.93.

tasked by SIRC to conduct a review of specific activities of CSIS, which will be referred to later under the section on SIRC).[26]

The history of relations between the IG, CSIS, and the Minister has been mixed, with occasional strains evident. The exception to access made for Cabinet confidences may be significant, in that the government treats Cabinet communications to CSIS as falling into this category, thus making the IG's job potentially difficult. One IG in the early 1990s objected to what she took to be unreasonable limitations on her access to CSIS records relating to ongoing investigations. The Minister supported the CSIS Director on this point, and this IG resigned her position after a relatively short tenure.[27] A number of ministerial directives and guidelines to CSIS have been made public, in whole or in part, via *Access to Information Act* releases, and SIRC reports. Those dealing with the handling of human sources – not covered by judicial controls over technical surveillance – and the targeting of so-called 'sensitive' institutions, such as universities and religious organizations, suggest that fairly strict guidelines are imposed on CSIS actions.[28]

### 3. Judicial control

Sections 21 to 28 of the *CSIS Act* lay out a relatively elaborate mechanism for applications for judicial warrants authorizing CSIS to carry out the interception of communications, the installation of surreptitious surveillance devices, entering of private premises, and search and seizure of documents, records, information, or any other "thing". Such applications must be made in writing and accompanied by an affidavit of fact indicating reasonable grounds for believing that the target may constitute a threat to security as defined in the Act, and that other, less intrusive, methods of investigation are likely to prove inadequate. The target, including the person or persons, the place, and the information or things sought, must be specified. Warrants

---

[26] There is one article from the late 1980s devoted to an analysis of the IG's role: Joseph Ryan, 'The Inspector General of the Canadian Security Intelligence Service,' *Conflict Quarterly*, IX:2 (Spring, 1989), pp. 33-51.

[27] Reg Whitaker, 'Designing a balance between freedom and security', in Joseph F. Fletcher, ed., *Ideas in Action: Essays on Politics and Law in Honour of Peter Russell* (Toronto: University of Toronto Press, 1999), p. 139.

[28] Memorandum, Solicitor General to Director of CSIS, 30 Oct. 1989. Solicitor General Canada, *On Course: National Security for the 1990s* (Ottawa: Supply & Services Canada, Feb. 1991), p. 14.

are also limited in duration, no more than one year,[29] although application may be made for renewal. There is no provision for later notifying the targets that they have been under surveillance.

Warrant applications are heard *in camera*. In 1987, early in CSIS's institutional history, however, a warrant application containing incorrect information led to the resignation of the first Director, and to the compromising of a case against conspirators planning to assassinate a visiting minister from a foreign government. Following that, and in part in response to earlier suggestions from SIRC on strengthening the warrant application process, CSIS has constructed elaborate, multi-step, internal control mechanisms for approval of applications.[30] This has led one observer to suggest that the main impact of the judicial control of surveillance applications may actually lie in the internalization of the control process within CSIS.[31]

Judicial review of CSIS actions may also apply in certain cases where SIRC decisions on security clearance complaints are appealed to the Federal Court, or where refugee claimants are issued security certificates that would lead to their deportation. On a number of occasions, the courts have overruled decisions made by SIRC that concurred with the advice of CSIS. In these cases as well, *in camera* and *ex parte* proceedings are the rule, excluding disclosure of evidence that might jeopardize national security. Critics have questioned the degree to which individual rights and fundamental justice are protected under such circumstances. The most extensive research into the practice of secret proceedings in Canada focuses on warrant application procedures and Federal Court review of national security cases. This study concludes that safeguards for rights have in many cases been incorporated by CSIS in its internal procedures[32], precisely to avoid judicial rebuke or public scandal, thus internalizing *Charter of Rights and Freedoms* values. The same study argues that "the Canadian procedures are among the most

---

[29] Sixty days only in the case of warrants sought under s. 2(d), the so-called 'subversion' definition of threats to security.

[30] See testimony of Jack Hooper, Factual Inquiry, pp. 458-473.

[31] Ian Leigh, 'Secret proceedings in Canada', *Osgoode Hall Law Journal* 34:1 (1996), p. 173.

[32] For a more recent overview, refer to the Testimony of Jack Hooper, Factual Inquiry, pp. 458-473.

innovative in the world for dealing with the eternal problem of reconciling state interests and individual rights."[33]

### 4. Independent review: SIRC

The *CSIS Act* established an independent review body, the Security Intelligence Review Committee (SIRC). Because of the significance of SIRC as a Canadian model for review of security and intelligence, the mandate and operations of SIRC are discussed in detail in the next section.

## D. THE SECURITY INTELLIGENCE REVIEW COMMITTEE

### 1. Membership

SIRC is constituted as a Committee consisting of a Chair and not less than two and not more than four members.[34] All of the members of the committee are Privy Councillors[35] not serving in Parliament. The statute provides that they are to be chosen by the Prime Minister after "consultation" with the Leader of the Opposition and the leaders of each party in the House of Commons with twelve or more members. The implication of this consultation, never actually spelled out, is that the membership of SIRC should broadly reflect the partisan makeup of the House, thus paralleling the representative role of the parliamentary committee that was not created. Mirror representation of Parliament, however, has not always been the case in practice.[36]

---

[33] *Loc cit.*

[34] *CSIS Act*, *supra* note 13. Section 34(1) establishes the criteria regarding the composition of SIRC.

[35] In practice, some SIRC members have been named Privy Councillors in order to assume office.

[36] Some members of SIRC have been politically independent. It has not been possible for SIRC to continue to mirror Parliament following major electoral changes in party representation, as after the 1993 General Election. There has never been a SIRC member appointed with past affiliation with the *Bloc Québécois* (although the leader of that party in the House has consulted over the appointment of members from the province of Québec). It took six years following the party's first appearance as an official party in the House of Commons, for the Reform/Canadian Alliance party to gain a representative on the Committee. SIRC has, however, always had one member with past affiliations to the New Democratic party.

Each member of SIRC is appointed for a five-year term during good behaviour, and is eligible to be reappointed for a term not exceeding five years.[37] The members of SIRC must comply with the security requirements applicable to employees under the *CSIS Act*, and are required to take an oath of secrecy.[38]

## 2. Overview: SIRC Mandate

SIRC is mandated to "review generally the performance by the Service (that is, CSIS) of its duties and functions".[39] In carrying out its review function, SIRC is entitled to have full access to all information it requires from CSIS and the IG, save Cabinet confidences.[40] Section 38(a) of the *CSIS Act* sets out certain aspects of the general review power, including:

(a) to review the reports of the Director and the certificates of the Inspector General with respect to the operational activities of the Service;

(b) to review directions issued by the Minister to the Service;

(c) to review arrangements entered into by the Service with provincial governments and departments and police forces in a province to provide security assessments, and to monitor the provision of information and intelligence pursuant to these arrangements;

---

[37] *CSIS Act*, *supra* note 13, s. 34(2) - (3).

[38] *Ibid.*, s. 37.

[39] *Ibid.*, s. 38.

[40] *Ibid.*, s. 39. There are two exceptions to complete access. SIRC, like the IG, is excluded from receiving cabinet confidences, including cabinet communications to CSIS. In 1988, SIRC entered into a 'Third Party-Access Protocol' with CSIS that potentially limits SIRC access to CSIS documents containing information provided by third parties (foreign governments and organizations) if the latter withhold consent, although CSIS "will use its best efforts to obtain authority to disclose information provided by third parties when requested to do so by SIRC". See Memorandum from Chairman of SIRC to Director of CSIS, 25 May 1988, with Annex of same date. In the mid-1990s, SIRC publicly complained when a CSIS document it had sought was instead returned to its donor agency: SIRC Report 1995-1996 (Ottawa, 1995) pp. 5-6.

(d) to review arrangements entered into by the Service with foreign governments and institutions, and international organizations of states and their institutions to provide security assessments, and to monitor the provision of information and intelligence pursuant to these arrangements;

(e) to review arrangements entered into by the Service and cooperation with departments of the federal government, or a provincial government and its departments, or a police force in a province, or governments of foreign states and their institutions, or an international organization of states and their institutions, and to monitor the provision of information and intelligence pursuant to these arrangements;

(f) to review reports by the Director of the Service where, in the Director's opinion, an employee of a service may have acted unlawfully;

(g) to monitor requests made to the Service by the Minister of National Defence or the Minister of Foreign Affairs to assist them, within Canada, in the collection of information or intelligence relating to foreign states and persons;

(h) to review the regulations, and

(i) to compile and analyse statistics on the operational activities of the Service.

Another important element of SIRC's mandate as set out in section 38(b) of the *CSIS Act* is to conduct reviews, or direct the Service or the IG to conduct reviews, to ensure that the activities of the Service are carried out in accordance with the Act, regulations and ministerial directions, and that the activities "do not involve any unreasonable or unnecessary exercise by the Service of any of its powers."[41] SIRC may task the IG to review particular matters, or "where it considers that a review by the Service or the Inspector General would be inappropriate, conduct

---

[41] *CSIS Act*, *supra* note 13, s. 40.

such a review itself."[42] In addition to matters which form part of SIRC's regular reviews, section 54 of the *CSIS Act* provides that SIRC may, on request by the Minister or at any other time, furnish the Minister with a special report concerning any matter that relates to the performance of its duties and functions. Since 1984, SIRC has made approximately thirty-seven section 54 Reports. These may include inquiries into particular allegations, such as a report to the Minister on the role of CSIS in relation to Maher Arar, or they may be more systemic in nature, such as the two 1998 Reports on CSIS cooperation with the RCMP.

SIRC has the mandate to investigate two categories of complaint pursuant to sections 41 and 42 of the *CSIS Act*. The first are complaints made with respect to "any act or thing done by the Service."[43] The second are complaints relating to the denial of security clearances for federal government employees or prospective employees, as well as for federal government contractors.[44]

SIRC also has a mandate to conduct investigations in relation to two categories:[45]

(a) reports made to SIRC by the Minister of Citizenship and Immigration pursuant to section 19 of the *Citizenship Act* regarding a proposal to refuse to grant citizenship or issue a certificate of renunciation on the basis that there are reasonable grounds to believe the person will engage in activities constituting a threat to Canada or are a part of a pattern of criminal activity to further the commission of an indictable offence; and

(b) matters referred to SIRC by the Canadian Human Rights Commission pursuant to section 45 of the *Canadian Human Rights Act*, where a Minister advises the

---

[42] *Ibid.*, s. 40.

[43] *Ibid.*, s. 41(a).

[44] *Ibid.*, s. 42.

[45] Prior to an amendment of the *CSIS Act* in 2001, SIRC also conducted investigations and hearings with respect to ss. 39 and 81 of the *Immigration Act*, recommendations of deportation where it is alleged that a person is either a security threat, or following conviction for a serious criminal offence, that they are involved in organized crime.

> Commission that the practice relating to a complaint under the Act is based on considerations relating to Canada's security.[46]

In preparing its Annual Reports, SIRC develops a research plan. SIRC states that because of its small size in relation to CSIS, it operates on the basis of risk management.[47] In addition to conducting a Regional office review or an audit of a Security Liaison Officer (SLO) post abroad, SIRC will also select topics for in-depth inquiries. SIRC has stated that the factors influencing its selection of such topics include:

- the nature of the international threat environment;
- public undertakings by SIRC to follow-up on past reviews or launch new ones;
- issues arising from complaints brought before SIRC;
- alterations in government policy or practice with significant implications for CSIS operations; and
- SIRC's statutory obligations under section 38 of the *CSIS Act*.[48]

In the 2002-2003 period, for example, SIRC undertook a review of regional investigations which it described as relating to "Sunni Islamic Extremism", and another review of the matter of Ahmed Ressam. In 2001-2002, the topics for in-depth inquiry included source recruitment and domestic extremism. In conducting these in-depth inquiries, SIRC typically reviews all relevant Service documents and files, electronic and hard-copy. These include targeting authorizations, warrants and their supporting documents, operational reports, human source logs, internal CSIS

---

[46] *CSIS Act*, *supra* note 13, s. 38(c).

[47] Security Intelligence Review Committee (SIRC) website, Reviews. Last updated January 31, 2004 <http://www.sirc-csars.gc.ca/reviews-e.html>.

[48] SIRC Report 2002-2003, (Ottawa, 2003) p. 4. Please note that all SIRC Reports were accessed online on the Annual Reports page of the SIRC website, last updated January 15, 2004 <http://www.sirc-csars.gc.ca/reports_e.html>.

correspondence, and records of exchanges of information with other agencies and departments including, where relevant, international agencies. SIRC may also conduct interviews.

In addition to such special topics, SIRC reports on other operational activities, investigation of complaints, CSIS accountability mechanisms, and inquiries under the *Access to Information* and *Privacy Acts*. Examples of how SIRC discharges its mandate are discussed below.

### *(i) Targeting*

Within CSIS, the Target Approval Review Committee (TARC) is the senior operational committee charged with considering and approving applications by CSIS officers to launch investigations.[49] TARC is chaired by the Director of CSIS, and includes senior CSIS officers as well as representatives from the Department of Justice and the Ministry of the Solicitor General.[50] SIRC reviews targeting authorizations made by TARC to ensure compliance with the *CSIS Act*, ministerial directions and relevant operational policies. SIRC annually reviews targeting authorizations in a selected Region as part of the Regional audit. It may also review targeting authorizations in the course of preparation of special reviews or reports.

In the conduct of its reviews, SIRC will examine issues such as:

- whether the Service had reasonable grounds to suspect a threat to the security of Canada in seeking its targeting approval,
- whether the level and intrusiveness of the investigation was proportionate to the seriousness and imminence of the threat,
- whether the Service collected only that information strictly necessary to advise the government of a threat,

---

[49] For an overview of TARC, see Testimony of Jack Hooper, June 22, 2004, Factual Inquiry, pp. 458-473.

[50] SIRC Report 1999-2000, (Ottawa, 2000), *supra* note 48, p. 13.

- in conducting its investigations, did the service respect the rights and civil liberties of individuals and groups, and

- information exchange with other agencies.[51]

An example of targeting review is reflected by SIRC's consideration of issues related to a form of investigation called "issue based" targeting. This type of targeting authorizes an investigation to take place in circumstances where CSIS suspects there is a threat to the security of Canada, but where the particular persons or groups associated with the threat have not been identified. The targeting authority allows CSIS to "investigate the general threat, and to try to identify the persons or groups who are taking part in threat-related activities."[52]

After reviewing the emergence of this issue in its 1998-1999 Report, SIRC determined that there was a place for issue-based targeting in the array of options legally available to CSIS, adding the caveat that investigations under such issue-based targeting authorities should be carefully monitored by senior management, and urging the Service to "make every effort to make the transition from issue-based to individual (identity-based) targeting as expeditiously as is reasonable".[53]

In 2002-2003, SIRC identified concerns regarding the termination of investigations in a timely manner if the activities of the target no longer constitute a threat. Therefore, in the 2002-2003 report, SIRC recommended that "CSIS maintain a strict awareness of operational policy and executive directive requiring the timely termination of targeting authorities in the absence of targets' threat-related activity.[54]

---

[51] SIRC Report 2002-2003, *supra* note 48, pp. 14-16.

[52] SIRC Report 2001-2002, *supra* note 48, p. 11.

[53] SIRC Report 1998-1999, *supra* note 48, p. 34.

[54] SIRC Report 2002-2003, *supra* note 48, p. 17.

### *(ii) Foreign Intelligence*

Foreign intelligence refers to the collection and analysis of information about the "capabilities, intentions or activities" of a foreign state. Under section 16 of the *CSIS Act*, at the written request of the Minister of Foreign Affairs or Minister of National Defence, and with the approval of the Solicitor General, the Service may collect foreign intelligence. The collection must take place in Canada, and cannot be directed against Canadians, permanent residents or Canadian companies.[55] As part of its annual review, SIRC examines all Minister's requests for section 16 operations. SIRC scrutinizes the Minister's requests to ensure compliance with the Act, as well as compliance with a Government Memorandum of Understanding to the effect that any request must contain an explicit prohibition against targeting Canadians, permanent residents and Canadian companies, and that the request should indicate whether the proposed activity is likely to involve Canadians.[56]

As part of the scrutiny under section 16, SIRC reviews working files on a randomly selected audit basis, in the course of which SIRC may identify errors. For example, in the 1997-1998 Report, SIRC reported on two errors. They identified that in one instance, CSIS had mistakenly intercepted the communications of a person for three days, although no information was collected or retained, and in a second instance, communications involving a Canadian national had been intercepted. SIRC also scrutinizes the appropriate retention of foreign intelligence for identifying the information or individuals.

One of the functions which SIRC performs is to routinely scrutinize CSIS requests to CSE to ensure that the requests are appropriate and that they comply with existing law and policy. The information that CSE routinely gives to CSIS is "minimized" in order to comply with the prohibition on the collection of information on Canadian nationals and Canadian companies. For example, the actual identity of a Canadian contained in CSE information provided to CSIS would be shielded by employing the phrase "a Canadian businessman". Under special

---

[55] *CSIS Act*, *supra* note 13, s. 16.

[56] SIRC Report, 1997-1998, *supra* note 48, p. 53.

circumstances, however, CSIS may request identities if it believes the information is relevant to an ongoing section 12 (threats to security) investigation.[57] In the 2000-2001 Report, for example, one request involved a prominent Canadian who had been approached by a foreign national, and the second request concerned a sensitive institution (trade union, media organization, religious body or university campus) involved in political campaigns in a foreign country. CSIS informed SIRC that the information was removed from its files following the SIRC review where the problem had been identified.[58]

Access to the foreign intelligence (section 16) database is restricted to those CSIS employees who have received special clearance and indoctrination. The foreign intelligence database is thus not routinely accessible to intelligence officers involved in section 12 investigations. As part of its review function, SIRC examines a random sample of correspondence related to the indoctrination of intelligence officers and their requests for access to the database to determine whether they are in compliance with this policy.

### *(iii) Foreign Arrangements*

In the context of foreign arrangements, SIRC reviews a number of aspects. It reviews written arrangements with foreign intelligence services, and the scope of cooperation with such services. In reviewing new arrangements or the expansion of existing arrangements, SIRC scrutinizes to determine that these are carried out in compliance with the *CSIS Act*, Ministerial directions and the Solicitor General's conditions for approval. SIRC also examines information relevant to the human rights record of the agency's host countries, including open-source reporting from reputable human rights agencies. SIRC flags relationships where CSIS must be vigilant in ensuring that no information received from an agency is the product of human rights violations, and that no intelligence transferred to a foreign agency results in such abuses. SIRC also examines the substance of information exchanged under any given foreign arrangement during

---

[57] SIRC Report 2000-2001, *supra* note 48, p. 27.

[58] *Ibid.*, p. 28.

the course of its regular reviews of individual Security Liaison Officer (SLO) posts abroad.[59] They will focus on a single CSIS SLO post for such review. They then review, in the context of the operation of the SLO post, the Service's relations with foreign security and intelligence agencies, the management of controls over the dissemination of CSIS information, post profiles and foreign agency assessments prepared by the SLO, the nature of the information collected and disclosed, and developments specific to the foreign agencies within that post's ambit.[60]

SIRC also scrutinizes information sharing. In the 1997-1998 Report, for example, it noted that CSIS had handled a request from a Canadian law enforcement agency to ask several allied intelligence services to conduct records checks on more than 100 people suspected of being involved in trans-national crime. SIRC found the grounds for some of these requests to be of doubtful validity, noting for example that one person about whom information was requested was said to have been "caught shoplifting".[61]

As part of its work, SIRC may identify situations where policies are silent or inadequate; in such cases, SIRC will make recommendations. For example, in 1997-1998, SIRC recommended that CSIS develop a policy regarding requests for the assistance of foreign agencies to investigate Canadian residents travelling abroad.[62]

### *(iv) Warrants*

CSIS annually reviews a number of aspects of the use by CSIS of Federal Court warrants, and it collects warrant statistics. As SIRC stated in its 2001-2002 Annual Report:

> Warrants are one of the most powerful and intrusive tools in the hands of any department or agency of the Government of Canada. For this reason alone, their use bears continued scrutiny, which task the Committee takes very seriously. In

---

[59] SIRC Report 2002-2003, *supra* note 48, pp. 22-23; see also SIRC Report 1997-1998, *supra* note 48, p. 22.

[60] SIRC Report 2001-2002, *supra* note 48, p. 16.

[61] SIRC Report, 1997-1998, *supra* note 48, p. 22.

[62] *Ibid*., p. 21.

> addition, our review of the Service's handling of warrants provides insights into the entire breadth of its investigative activities and is an important indicator of the Service's view of its priorities.[63]

SIRC examines a number of aspects relating to warrants including warrant acquisition, warrant implementation, applicable court decisions and regulations, and warrant statistics.

In reviewing the obtaining of a warrant, SIRC examines all documents relating to how the warrant applications were prepared including the affidavits and supporting documentation, working files relating to the affidavit, the requests for targeting authority, and the Target Approval Review Committee (TARC) minutes. In reviewing this documentation, SIRC seeks to ascertain whether:

- the allegations and the affidavits are factually correct and adequately supported in the documentation;
- all pertinent information is included in the affidavits; and
- the affidavits are complete and balanced, and the facts and circumstances of the cases are fully, fairly and objectively expressed.[64]

In its 1998-1999 Annual Report, for example, SIRC reviewed three applications in a region relating to two target groups in the counter-terrorism area. In its review, SIRC stated that "we identified a number of statements made by the Service which accurately reflected neither the operational nor the open source information available to the Service".[65]

In terms of warrant implementation, SIRC reviews active warrants in a Region to ensure that the warrant powers were implemented properly, to assess the use of powers granted in the warrant

---

[63] SIRC Report 2001-2002, *supra* note 48, p. 48.

[64] *Ibid.*, p. 21.

[65] SIRC Report 1998-1999, *supra* note 48, p. 39.

and to determine whether CSIS complied with all clauses and conditions contained in the warrants. SIRC also determines whether or not in its implementation, the Service meets the "strictly necessary" test set out in section 12 of the *CSIS Act* in terms of both collecting and retaining information.

### *(v) Complaints*

As set out above, SIRC also investigates complaints with respect to four categories:

- complaints "with respect to any act or thing done by the Service" as described in the *CSIS Act*;
- complaints about denials of security clearances to federal government employees and contractors;
- matters referred by the Canadian Human Rights Commission where the complaint raises considerations relating to Canada's security; and
- Minister's reports in respect of the *Citizenship Act*.

Examples of the kinds of complaints that SIRC investigates with respect to section 41, "any act or thing", include:

- allegations of unreasonable delay in conducting a security screening investigation;
- allegations that CSIS provided adverse and inaccurate information to foreign authorities;
- allegations that CSIS failed to investigate threats to the security of Canada; and
- allegations of improper investigation of lawful advocacy, protest and dissent.

Since the inception of SIRC, it has received 943 complaints (excluding those dealing with the application of the *Official Languages Act* in the workplace)[66]. The total number of complaints does not mean that SIRC will accept jurisdiction to investigate all of them. The Review Committee first performs a preliminary review to determine whether it has jurisdiction. Some complaints may not be within SIRC's mandate. Others may be resolved without an investigation. SIRC may not accept jurisdiction under section 41 of the *CSIS Act* if it determines that the complaint is trivial, frivolous, vexatious or made in bad faith, or that the complaint is subject to a grievance procedure established under the *CSIS Act* or the *Public Service Staff Relations Act*.[67] SIRC has produced 118 written reports following investigations of complaints, involving either a written or oral hearing.[68]

Where a complaint proceeds to a hearing, there are special procedures set out in the *CSIS Act* and SIRC's procedural rules[69] designed to balance the individual's procedural fairness interests with the government's national security concerns.

After SIRC has determined that it has jurisdiction under section 42 (security clearance denial) to investigate the complaint, it must send a statement to the complainant summarizing information available to SIRC "as will enable the complainant to be as fully informed as possible of the circumstances giving rise to the denial of the security clearance".[70] Where the Canadian Human Rights Commission refers a complaint to SIRC, SIRC must also provide a statement to the

---

[66] Between 1985 and 1987, SIRC received 2,256 complaints with respect to the application of the *Official Languages Act* in the workplace, bringing the total to 3,199 complaints (Information provided by SIRC October 15, 2004).

[67] *CSIS Act, supra* note 13, s. 41.

[68] Information provided by SIRC, October 8, 2004.

[69] Rules of Procedure of the Security Intelligence Review Committee in Relation to its function under paragraph 38(c) of the *CSIS Act*, June 1985, s. 46(2) ("SIRC Rules of Procedure").

[70] *CSIS Act, supra* note 13, s. 46.

complainant summarizing the information available to it on the circumstances giving rise to the referral.[71]

Investigations of complaints are conducted *in camera*. SIRC has the power to summon witnesses, to compel documents to be produced, and to administer oaths.[72] The complainant, CSIS and relevant departments are all given the right to make representations to SIRC, to present evidence, and to be represented by counsel. The *CSIS Act* provides, however, that "no one is entitled as of right to be present during, to have access to, or to comment on representations made . . . by any other person".[73]

SIRC's Rules of Procedure applicable to all its investigations provide for discretionary disclosure of evidence and representations to parties, subject to s. 37 of the *Act*. The SIRC Rules of Procedure provide that it is within the discretion of the member conducting the investigation, in "balancing the requirements of preventing threats to the security of Canada and providing fairness to the person affected"[74], to disclose the representations of the parties to one another.

SIRC's Rules of Procedure provide a similar discretion to determine whether a party may cross-examine witnesses called by other parties, and to exclude parties during the giving of evidence.[75] In the case of an *ex parte* hearing (where parties are excluded), SIRC counsel will cross-examine witnesses. As one commentator notes:

> [S]ince committee counsel has the requisite security clearance and has had the opportunity to review files not available to the complainant's counsel, he or she is

---

[71] *Canadian Human Rights Act*, R.S. 1985, c. H-6, s. 46(5).

[72] *CSIS Act*, *supra* note 13, s. 50.

[73] *Ibid.*, s. 48(2).

[74] SIRC Rules of Procedure, *supra* note 69, s. 46(2).

[75] *Ibid.*, s. 48(2)-(3).

> also able to explore issues and particulars that would be unknown to the complainant's counsel.[76]

When a party is excluded from a hearing for reasons of national security, he or she may, in the discretion of the presiding member and subject to s. 37 of the *Act*[77], and after consultation with the Director of CSIS, be provided with the substance of the evidence given or representations made.

The Supreme Court of Canada has considered the SIRC Rules of Procedure. The Court has held that the rules recognize and strike a fair balance between the competing interests of the individual in fair procedures, and the state interest in effectively conducting national security and criminal intelligence investigations and in protecting police sources.[78] An individual should be given sufficient information to know the substance of the allegations and be able to respond. Details such as criminal intelligence investigation techniques and police sources were not required to be disclosed in this case.

The McDonald Commission had recommended the creation of a separate Security Appeals Tribunal, presided over by a Federal Court judge, to hear appeals relating to immigration, citizenship and security clearances.[79] The McDonald Commission clearly contemplated that the hearing function would be separate from other review functions, stating:

> The Security Appeals Tribunal is a quasi-judicial body whose function would be to hear cases in which persons wish to challenge security clearance decisions. Given the adversarial nature of proceedings before the tribunal, and the need for the tribunal to function as much as possible like a Court, we think it should be

---

[76] Murray Rankin, "The Security Intelligence Review Committee: Reconciling National Security with Procedural Fairness", 3 C.J.A.L.P. 173, at pp. 182-185.

[77] *CSIS Act, supra* note 13., s. 48(4)-(5).

[78] *Canada (Minister of Employment and Immigration) v. Chiarelli*, [1992] 1 S.C.R. 711. This was a case involving the review of the deportation of a permanent resident based on alleged links with organized crime. Although national security information was not involved, the court's reasoning is equally applicable.

[79] See McDonald Commission Report, Vol. 1 at 421-26 and Vol. 2 at 805-811.

> quite separate from the Advisory Council on Security and Intelligence which will have a broad mandate to review and advise the government on all aspects of security and intelligence policy and operations.[80]

In the *CSIS Act*, however, the two functions – review and complaint hearings - are combined in the same body. Combining the two functions in one body does offer certain advantages from the point of view of accountability, offering SIRC a more comprehensive understanding of CSIS operations than would be possible if it were limited to the review function only. One author, based on interviews in the mid-1990's with CSIS and SIRC personnel, noted:

> In interviews, CSIS personnel described the effect of this interrelationship on complaints proceedings as "schizophrenic". The criticism was that case hearings had a tendency to turn into review hearings as SIRC pursued items of interest which related to policy and oversight, but which were beyond the scope of the complainant's case. SIRC, on the other hand, stressed the usefulness of the interrelatedness of the functions: in view of the part-time involvement of members of SIRC, complaints hearings were seen as a crucial means by which the members (rather than the permanent staff) obtained an insight into the operational work of CSIS. Counsel to SIRC confirmed that, on occasion, reviews had grown out of case hearings. Occasionally, the reverse has happened: for instance, when a SIRC report criticizing CSIS interviews with Palestinians during the Gulf War was published, . . . it led to an individual complaint about CSIS action from one of the interviewees concerned.[81]

### 3. Reporting by SIRC

SIRC must submit an annual report to the Minister, which is to be laid before Parliament.[82] Reports to Parliament are edited to protect national security and personal privacy, and are available in edited form on the SIRC website.[83] SIRC reports on both its review and complaint investigation functions. SIRC has powers to make findings and recommendations only; it does

---

[80] McDonald Commission Report, Vol. 2 at 883.

[81] Ian Leigh, "Secret Proceedings in Canada" (1996), 34 Osgoode Hall LJ, 113 at 160.

[82] *CSIS Act*, *supra* note 13, s. 53.

[83] See www.sirc-csars.gc.ca.

not have the power to make binding decisions. The Supreme Court has held that such recommendations are not binding on the government.[84]

SIRC may, either at the request of the Minister or at its own initiative, "furnish the Minister with a special report that relates to the performance of its duties and functions."[85] Under this latter rubric, 'section 54', SIRC has produced approximately thirty-seven special reports, some on relatively high profile issues that have come before the public, such as the Air India tragedy, the Heritage Front affair, and the role of CSIS in relation to Maher Arar.

## 4. SIRC and CSIS: two decades of evolution in the review process

Two decades have passed since the *CSIS Act* came into effect. During this period, the accountability features have been tested, and the relationship between SIRC and CSIS has evolved with experience. The context within which both the agency and its review body operate has changed dramatically, with important consequences for the role of security intelligence and national security accountability in the Canadian political system.

### *(i) 1984-1989/90:*

The first half decade of the *CSIS Act* fell within the continuing context of the Cold War, and the persistent assumption that the main security threat to Canada was from the Soviet Bloc and Communism. Counter-espionage was a leading priority for CSIS. Counter-subversion – a priority throughout the earlier Cold War period – was increasingly being questioned, a process to which SIRC contributed through its critical reviews of the Service's operations, leading in 1987 to the closure of the counter-subversion branch of CSIS on ministerial order.[86] Counter-

---

[84] *Thomson v. Canada (Deputy Minister of Agriculture)*, [1992] 1 S.C.R. 385.

[85] *CSIS Act*, *supra* note 13, s. 54.

[86] SIRC Report 1986-1987 (Ottawa, 1987), pp. 33-40. The impetus for closing the Branch also came from a special task force headed by a senior public servant, Gordon Osbaldeston: *People and Places in Transition*, Report to the Solicitor General of the Advisory Team on the Canadian Security Intelligence Service (October 1987. In general, see Peter Gill, 'Symbolic or real? The impact of the Canadian Security Intelligence Review Committee, 1984-1988', *Intelligence and National Security* 4:3 (July 1989) pp. 550-75.

terrorism became a leading concern as well, especially after the Air India bombing in 1985 took the lives of 329 people, most of them Canadians. The failure to prevent that attack, the shortcomings of the investigation (criminal proceedings only began in 2003), and evidence of lack of co-operation between CSIS and the RCMP, all contributed to heightened demands for greater accountability.[87]

### *(ii) 1990-2001:*

The post-Cold War decade was one of flux and transition for CSIS and for security intelligence generally. With the collapse of the Communist Bloc, and the end of the Soviet Union, the old paradigm had disappeared, but in this decade there was no clear successor paradigm to replace the old one. Government economy was being extended to encompass security and intelligence as well as other functions, and CSIS found its budget under constraint at the same time as they were having to redefine their role in a changing threat environment. In 1994, SIRC was called upon to undertake a major public accounting of a scandal that beset CSIS. The so-called 'Heritage Front affair' involved the naming in the media of a CSIS source within an extreme right-wing organization and a series of questions that arose from this revelation. SIRC was called upon by the Solicitor General to effect a 'Section 54' special investigation that was made public (with a few parts removed on security grounds).[88] This was a major exercise in transparent accountability, and one that was on the whole successful. Two additional developments in 1996 extended new accountability mechanisms: a Commissioner was appointed as an external reviewer for the Communications Security Establishment (CSE); and the Auditor General initiated the first in a series of audits of the intelligence community. Both these developments are discussed in greater detail below.

---

[87] A critical journalistic account of SIRC's relationship to CSIS in this era is Richard Cleroux, *Official Secrets: the Story Behind the Canadian Security Intelligence Service* (Scarborough: McGraw-Hill,1990).

[88] SIRC, *The Heritage Front Affair*, Report to the Solicitor General (9 Dec. 1994).

***(iii) 2001-present:***

The third phase was initiated by the terrorist attacks of September 11, 2001 on New York and Washington DC, and the declaration of a global 'War on Terrorism' in which Canada is a participant. New powers to combat terrorism were passed by Parliament; new resources have been invested; CSIS has stepped up its foreign intelligence gathering capacity; other agencies, including the RCMP and the CSE, have become more active in anti-terrorist activities, new players have joined the intelligence community; a new umbrella department of government, Public Safety and Emergency Preparedness Canada, has been created to direct the security and intelligence functions of government; and a National Security Policy has been published. Since Sept. 11, 2001, there has been no change in the accountability and review mechanisms to which CSIS is subject.

Institutionally, SIRC has moved over the years from an early period of relatively aggressive behaviour in establishing itself in relation to CSIS and defining its role (under the leadership of SIRC's first Chair, the Hon. Ronald Atkey, from 1984 to 1989), to a period of contraction and flux in the early 1990s, to a period of reconsolidation under the current Chair since 1996, the Hon. Paule Gauthier. The public perception of SIRC's effectiveness may be hampered by the degree to which most of its review activities are necessarily undertaken in secrecy, or semi-secrecy. Its public annual reports are only partially informative, and rarely attract much media or public attention. Occasional special Section 54 reports may cover topics of public concern, but are usually entirely or mostly classified, with only occasional glimpses coming to light through *Access to Information Act* requests. Some observers have suggested that SIRC's main impact may be found in the internal procedures and 'culture' of CSIS, reflecting an internalization of some of the norms of accountability that SIRC has advanced, and in the ability of CSIS to avoid pitfalls and usually stay out of trouble, partly as a result of external review of its operations.[89]

---

[89] See for instance Peter Gill, 'Symbolic or real?', op. cit. Laurence Lustgarten and Ian Leigh, *In From the Cold: National Security and Parliamentary Democracy* (Oxford: Oxford University Press, 1994), p. 461 write that SIRC "has pushed CSIS into what was described as 'pre-emptive change'. That is, CSIS has done things it would probably not have done, sometimes in more radical fashion than SIRC itself might have suggested. The very existence of a review body pushed the Service into integrating into its own decision-making the kinds of considerations SIRC exists to voice publicly." On the concept of an organizational culture in intelligence agencies, see Stuart Farson,

One of the questions that arises regarding the legislative framework for accountability in the *CSIS Act*, is whether there would be advantages to develop an external review body with wide responsibilities for the entire Canadian intelligence community. The *CSIS Act* establishes accountability on an institutional, rather than a functional basis. This has a number of consequences. CSIS has a relatively elaborate and demanding set of review mechanisms embedded in its statutory mandate and in its day to day operations. Other agencies, such as the RCMP and the CSE, have different external accountability requirements. The result is a fragmented system of review. This feature is of particular interest in view of the increasing integration of agencies involved in national security activities.

When SIRC was created in 1984, it was considered an innovative model for other countries. Today, some other countries have established arguably similar statutory mandates and controls for their intelligence community. For instance, in the United Kingdom, two leading intelligence agencies are regulated by the 1994 *Intelligence Services Act*[90]; and a third is regulated by the *Security Service Act 1989*. The 2000 Regulation of *Investigatory Powers Act* sets statutory limits on the use by these intelligence (and other) agencies of certain intelligence-gathering methods. The UK System of review and accountability is discussed in detail in the background paper entitled "International Models of Review and Oversight of Police Forces and Security Intelligence Agencies".

## E. THE CSE COMMISSIONER

### 1. Introduction

The Communications Security Establishment (CSE) is Canada's national cryptologic agency. It is restricted to technical, rather than human source based intelligence. The CSE intercepts,

---

'Old wine, new bottles and fancy labels: the rediscovery of organizational culture in the control of intelligence', in Greg Barak, ed., *Crimes by the Capitalist State: an Introduction to State Criminality* (New York: State University of New York Press, 1991), pp. 185-217.

[90] These are the Secret Intelligence Service or MI6, which gathers foreign intelligence, and the Government Communications Headquarters (the equivalent of the CSE).

decrypts where necessary, retains, and analyses foreign communications. Its mandate is set out in Part V.1 of the *National Defence Act* as follows: [91]

> (a) to acquire and use information from the global information infrastructure for the purpose of providing foreign intelligence, in accordance with Government of Canada intelligence priorities;
>
> (b) to provide advice, guidance and services to help ensure the protection of electronic information and of information infrastructures of importance to the Government of Canada; and
>
> (c) to provide technical and operational assistance to federal law enforcement and security agencies in the performance of their lawful duties.

CSE had its genesis in 1941 as part of the allied World War II effort. It was known as the Examination Unit and was located in the National Research Council. In 1946, it was renamed the Communications Branch, National Research Council (CBNRC). It was given responsibility for signals intelligence (SIGINT) and communications security (COMSEC) (now Information Technology Security or ITS). In 1975, CBNRC was renamed the Communications Security Establishment and by Order in Council was transferred to the department of National Defence.[92] However, it was not until September 22, 1983 that the existence and functions of the CSE were publicly acknowledged on behalf of the Government by the Hon. Jean-Luc Pepin, then Minister of State (External Relations), before the Special Committee of the Senate on the Canadian Security Intelligence Service.[93] This acknowledgement (known as "the Avowal") was made during the debate on the Bill that subsequently became the *CSIS Act*.

As early as 1990, the Parliamentary Committee charged with the five year review of the *CSIS Act* recommended that Parliament provide the CSE with a statutory basis as well as a review mechanism, a call later reiterated by the Privacy Commissioner in 1996 and the Auditor General in 1998. In the 1990s, rising criticism of the opacity of CSE operations, and unverified media

---

[91] *National Defence Act*, R.S. 1985, c. N-5, s. 273.64.

[92] P.C. 1975-95, C. Gaz. 1975 II, 233.

[93] Proceedings of the Special Committee of the Senate on the Canadian Security Intelligence Service, Hansard, September 22, 1983, at pp. 18-19, 27, and 31-33.

reports alleging wrongdoing, led the government of the day to appoint a CSE Commissioner by Order in Council to review the activities of the CSE and report annually to the Minister of National Defence on the lawfulness of those activities.[94] The government did not extend the mandate of SIRC to cover the CSE, as had been called for by the House of Commons Special CSIS Review Committee. It also did not provide a statutory mandate, an omission regularly observed by the CSE Commissioner himself in his annual reports.[95] In 1999, the Commissioner's mandate was extended to encompass a complaints investigation component as well, and the CSE's and CSE Commissioner's mandates were formalized by statute in 2001. This section will outline the path that led to the creation of the Commissioner's office, the current basis of its authority, and its mandate.

## 2. History of CSE Review Proposals

In 1993, analyst Philip Rosen described the CSE as "Canada's most secret intelligence agency."[96] At that time, unlike either CSIS or the RCMP, the CSE had no statutorily defined mandate. Although control and supervision of the CSE was transferred to the Department of National Defence by Order in Council in 1975,[97] details of its mandate, budget and activities remained largely confidential[98]. Therefore, what control mechanisms may have been in place did not involve public scrutiny of any form.

Over time, the government received and considered various recommendations for review of the CSE. In 1981, the McDonald Commission recommended that an Advisory Council on Security and Intelligence be established, with the power to review all non-police federal government

---

[94] 'CSE External review mechanism', Government of Canada news release NR-96.061, 19 June 1996.

[95] See for example, CSE Commissioner, *Annual Report 2001-2002* (Ottawa 2002), pp. 3-4.

[96] Library of Parliament Parliamentary Research Branch, "The Communications Security Establishment – Canada's Most Secret Intelligence Agency" by Philip Rosen in *Background Papers*, BP-343E (September 1993).

[97] P.C. 1975-95, C. Gaz. 1975.II. 233.

[98] Jeffrey T. Richelson and Desmond Ball, *The Ties that Bind – Intelligence Co-operation between the UKUSA Countries*, 2nd edition (Boston: Unwin Hyman, 1990) 89, cited in Rosen, *supra* note 95, p. 4.

organizations that collect intelligence through clandestine means.[99] This was not explicitly acknowledged to encompass the CSE. In 1990, the House of Commons Special CSIS Review Committee recommended that the CSE be established by statute and made subject to review by the Security Intelligence Review Committee.[100] In response, the government summarized the "broad accountability system" then in place for the CSE as follows: the Minister of National Defence was accountable to Parliament for the CSE, and approved major capital expenditures, long-term plans, and major initiatives; the Chief of CSE was accountable to the Deputy Minister of National Defence for financial and administrative matters, and to the Deputy Clerk (Security and Intelligence, and Counsel) in the Privy Council Office for policy and operational matters; Department of Justice counsel provided advice to the CSE; CSE consulted with senior officials in relevant ministries; CSE was subject to internal administrative review mechanisms of the Department of National Defence; and CSE submitted a strategic plan and new policy proposals to an Interdepartmental Committee on Security and Intelligence.[101] The government acknowledged that the system could always be improved and that in due course a decision would be taken on the "most appropriate approach."[102] The CSE was subject to review by various external bodies, such as the Canadian Human Rights Commission, the Privacy Commissioner, the Information Commissioner, the Commissioner of Official Languages, and the Auditor General of Canada. However, as the Auditor General observed in 1996, such review was "of necessity, both intermittent and narrow in scope" due to the specific mandates of the review bodies and the limitations flowing from the need to secrecy around many CSE activities.[103]

---

[99] Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police, *Freedom and Security under the Law, Second Report*, vol. 2 (Ottawa: Supply and Services Canada, 1981) 885.

[100] House of Commons Special Committee on the Review of the *Canadian Security Intelligence Service Act* and the *Security Offences Act, In Flux but not in Crisis – The Review of the Canadian Security Intelligence Service Act and the Security Offences Act* (Ottawa: House of Commons Special Committee on the Review of the *Canadian Security Intelligence Services Act* and the *Security Offences Act*, 1990).

[101] Solicitor General of Canada, *On Course: National Security for the 1990s* (Ottawa: Supply and Services Canada, 1991) 54-55.

[102] *Supra* note 7, p. 55.

[103] Auditor-General of Canada, "The Canadian Intelligence Community: Control and Accountability," in *1996 Report of the Auditor General of Canada* (Ottawa: Auditor General of Canada, 1996) 27.53.

### 3. Establishment of CSE Commissioner

In June 1996, the office of the Communications Security Establishment Commissioner was created, with the appointment of the first Commissioner, the Hon. Claude Bisson, former Chief Justice of Québec. The Commissioner was appointed by an Order in Council under Part II of the *Inquiries Act*.[104] He was appointed for a three-year term, subsequently renewed,[105] "to review the activities of the [CSE] to determine whether those activities are in compliance with the law."[106] Therefore, the Commissioner could review the CSE's activities for compliance with the *Criminal Code*, the *Charter of Rights and Freedoms*, the *Privacy Act*, or any other relevant legislation. This is still the case. Because the Orders in Council specified the Commissioner by name, no qualifications required for appointment to the position were set out. The Commissioner was directed to submit a report annually to the Minister of National Defence regarding his activities and any unclassified findings, to be tabled in Parliament; in addition, he was empowered to submit classified reports to the Minister "at any time the Commissioner consider[ed] it advisable."[107] Furthermore, the Commissioner was directed to inform the Minister and the Attorney General of any CSE activity that the Commissioner believed might not comply with the law. From 1999, the terms of appointment shifted to authorize the Commissioner to inform any complainant of the results of his investigation, while not disclosing any classified information in the process of doing so.[108] Previously, a complainant would have received only as much information about the resolution of his or her complaint as was provided in the annual report tabled in Parliament.

From 1996 to 2001, the Commissioner undertook review activities as authorized by the appointing Orders in Council. In practice, the Commissioner's annual reports have outlined in

---

[104] P.C. 1996-899.

[105] P.C. 1999-1048.

[106] P.C. 1996-899.

[107] P.C. 1996-899.

[108] P.C. 1999-1048.

broad terms whether any complaints were received and whether any complaints were found to have merit, as well as the results of reviews undertaken in various areas of operation, for example, the exchange of information with other countries or internal controls on activities. The annual report has also included a cumulative list of classified reports made to the Minister, with classified information removed from the titles.

Following the creation of the Commissioner's position, the Commissioner and commentators continued to recommend a statutory framework for the CSE's authority and the Commissioner's own mandate. Reviews by the Privacy Commissioner and the Auditor General in 1996 both recommended the enactment of a legislative framework for the CSE.[109] The Auditor General observed that the newly created Commissioner's mandate focussed entirely on compliance with the law, and represented an "important step towards enhancing CSE's public accountability," through his work, which should include increasing "the scope for informed parliamentary scrutiny and debate."[110] In 1999, the Senate Committee on Security and Intelligence recommended that the CSE have its own Act of Parliament, providing for a permanent and separate review body.[111] The Commissioner also expressed the view in his annual reports that enabling legislation would be beneficial. In his 1999-2000 annual report, for example, he described legislation as an "appropriate development," but also noted that current arrangements were "entirely effective," and that there was "no urgency to alter them independent of the larger issue of whether CSE should have a legislative base."[112]

---

[109] Privacy Commissioner of Canada, *Annual Report 1996* (Ottawa: Privacy Commissioner of Canada, 1996); Auditor-General of Canada, "The Canadian Intelligence Community: Control and Accountability," in *1996 Report of the Auditor General of Canada* (Ottawa: Auditor-General of Canada, 1996) 27.50.

[110] 1996 Report of Auditor-General, *supra*, note 15, p. 27.65.

[111] Communications Security Establishment Commissioner, *Annual Report 2001-2002* (Ottawa: Communications Security Establishment Commissioner, 2002) 3.

[112] Communications Security Establishment Commissioner, *Annual Report 1999-2000* (Ottawa: Communications Security Establishment Commissioner, 2000) 12.

## 4. Current Mandate of the CSE Commissioner

The events of 9/11 created a new sense of urgency regarding protection of both security and freedoms. Among the many legislative amendments contained in the *Anti-terrorism Act* passed in December 2001, the role of the CSE and the CSE Commissioner were finally provided for in legislation. The basis for the authority of the Commissioner is now found in two statutes. Section 273.63(1) of the *National Defence Act* provides that the Governor in Council may appoint a supernumerary judge or a retired judge of a superior court as Commissioner of the Communications Security Establishment for a term of not more than five years.[113] The Act continues the requirement of submitting an annual report to the Minister on the Commissioner's activities and findings, to be tabled before Parliament.[114] It is specified that in carrying out his or her duties, the Commissioner continues to have all the powers of a commissioner under Part II of the *Inquiries Act*, for example the power to summon witnesses and to hear evidence under oath.[115] The Commissioner is empowered to engage the services of legal counsel, technical advisers and assistants, and to fix and pay their remuneration with the approval of the Treasury Board.[116]

The *National Defence Act* provides the CSE Commissioner with both a review function and a complaints function. The duties of the Commissioner are described as:

(a) to review the activities of the CSE to ensure that they are in compliance with the law;

(b) in response to a complaint, to undertake any investigation that the Commissioner considers necessary; and

---

[113] *National Defence Act*, R.S.C. 1985, c. N-5, s. 273.63(1).

[114] *Supra*, note 19, at s. 273.63(3).

[115] *Supra*, note 19, at s. 273.63(4).

[116] *Supra*, note 19, at s. 273.63(5).

(c) to inform the Minister and the Attorney General of Canada of any activity of the Establishment that the Commissioner believes may not be in compliance with the law.[117]

### *(i) Review Duties*

To carry out his review function, the Commissioner has full access to CSE information holdings.[118] The Commissioner monitors control and accountability mechanisms, the scope and application of policies and procedures, employee training programs, internal investigations and complaints, use and retention of collected information, and use of technology.[119] The *Anti-terrorism Act* expanded the CSE's role of collecting foreign intelligence to permit the Minister of National Defence to authorize interception of private communications of Canadians in certain circumstances and providing certain conditions are met.[120] In doing so, the Minister must be satisfied that measures taken by the CSE will protect Canadians' privacy. The Commissioner is specifically directed to review activities carried out under each ministerial authorization to ensure that they comply with the authorization, and to include his or her findings in the annual review.[121] In the 2003-2004 Annual Report, the Commissioner reported on a general issue "about the structure and process for using ministerial authorizations", noting that "[c]ertain weaknesses in policies and procedures related to these activities were brought to CSE's attention", and that some issues had been resolved while others remained.[122] The Commissioner

---

[117] *Supra*, note 19, s. 273.63(2).

[118] The CSE Commissioner takes the position that nothing in Part V.1 of the *National Defence Act* or the *Inquiries Act* precludes the Commissioner from accessing information holdings protected by Cabinet privilege: Information provided by the Office of the CSE Commissioner, November 24, 2004.

[119] Communications Security Establishment Commissioner, "Review Function," online: The Office of the Communications Security Establishment Commissioner < http://www.csec-ccst.gc.ca/functions/review_e.php >.

[120] *National Defence Act, supra* note 62, s. 273.65.

[121] *Supra*, note 19, ss. 273.65(1) and (3).

[122] Communications Security Establishment Commissioner, *Annual Report 2003-2004* Ottawa: Communications Security Establishment Commissioner, 2004), page 9.

has expressed cautious optimism that the difficulties "in providing meaningful assurance in respect of CSE's activities under Ministerial authorization will be addressed by the end of 2004.

Although he is no longer explicitly required to do so the Commissioner has continued the practice of providing the Minister with reports containing classified information whenever he considers it advisable. The Commissioner observed in his 2002-2003 annual report that he would continue "reporting practices [that] have served well in the past."[123] The review function is multi-faceted and expanding, including but not necessarily limited to *post facto* case-specific review.

### *(ii) Complaints Duties*

To trigger the Commissioner's complaints function, any Canadian citizen or permanent resident of Canada can file a complaint regarding the lawfulness of CSE activities. Complaints will not be dealt with if they are frivolous, vexatious or made in bad faith. The Commissioner will not deal with a matter for which there are other avenues of redress, or with a matter that arose with the complainant's knowledge more than a year before the complaint was filed. After a complaint is filed, the Commissioner decides the action to be taken based on the recommendations of a Complaints Review Committee. At this stage, conflict resolution methods may be used to resolve the complaint. If a formal investigation ensues, the Commissioner informs the complainant, the Chief of the CSE, and the Minister of National Defence, and assigns an investigator. Following an investigation, the Commissioner prepares an interim report with findings and recommendations. The Chief of CSE may be asked to respond with details of responses to the report. Then the final report is prepared and submitted to the Chief of CSE and the Minister. The complainant is then advised in writing of the results of the investigation.[124]

---

[123] *Supra*, note 26, p. 5.

[124] Communications Security Establishment Commissioner, "Complaints Procedure," online: The Office of the Communications Security Establishment Commissioner <http://www.csec-ccst.gc.ca/functions/complaints-proceed_e.php>.

### *(iii) "Public Interest Defence" Duties*

In addition to the review and complaints functions of the Commissioner's office, a third function is now rooted in section 15 of the *Security of Information Act*.[125] The *Security of Information Act* prohibits anyone "permanently bound to secrecy" from communicating or confirming "special operational information," which would include information about CSE activities. If an individual bound by secrecy releases classified information about the CSE, he or she may seek to defend this action on the grounds that the public interest in disclosure outweighs the public interest in non-disclosure. To raise this defence to a charge under the Act, the individual must show that he or she followed a series of legislated steps before disclosing the operational information. The first step is to bring concerns to the attention of the institution's deputy or the Deputy Attorney General of Canada. If no reply is received within a reasonable time and the matter relates to the CSE, the individual must then bring the concern to the Commissioner and allow a reasonable time for response. It remains to be seen what steps the Commissioner might take in response to such a situation.

## F. THE AUDITOR GENERAL

The McDonald Commission had made a brief reference to the desirability of ensuring national security financial accountability through the office of the Auditor General. There was no specific provision for financial audits in the *CSIS Act*, but in the late 1990s, in a context of cost-consciousness and systematic program review in the federal government, the Auditor General initiated the first ever audit of Ottawa's security and intelligence functions as a whole. This report,[126] clearly indicated as the first of a regular cycle, was unprecedented in scope. The US General Accounting Office has audited specific programs, but never the entire field of intelligence. It was highly specific in recommendations for tightening controls and modifications to address indicated weaknesses. These features have been carried on in later reports, the most recent being a critical audit of the effectiveness of the anti-terrorism initiatives

---

[125] *Security of Information Act*, R.S. 1985, c. O-5, s. 15; c. 47, s. 80; 2001, c. 41, s. 29.

[126] Canada, *Report of the Auditor General of Canada to the House of Commons*, Chapter 27: 'The Canadian Intelligence Community – control and accountability' (Ottawa: Nov. 1996).

post-9/11, which received wide publicity in and out of Parliament.[127] Particularly noteworthy is that the Auditor General is an officer of Parliament, who reports to the Public Accounts Committee of the House of Commons. In recent years, reports from Auditor General's office have attracted increasing attention and governments appear to be under more pressure than in the past to respond positively to shortcomings revealed by the audits. The Auditor General is specifically mandated to examine financial controls, cost effectiveness of government operations, and standards of public service ethics in handling the taxpayers' dollars. The question thus arises whether financial audits should be included in a comprehensive review process and, if so, by whom.

In November 2003, the Auditor General released a report specifically directed to determining if there are gaps in the extent and nature of the external review of Canada's security and intelligence agencies, and in the disclosure of findings. The Auditor General assessed the level of external independent review over each agency involved either directly or in providing assistance with the collection of intelligence within Canada, including CSIS, the RCMP, National Defence, the CSE, the Canada Customs and Revenue Agency (CCRA)[128], and the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC).

The Auditor General concluded that powers to review security and intelligence agencies vary widely.[129] With respect to the Canadian Forces, the CCRA, and FINTRAC, the Auditor General noted that the organizations do not have a specific agency to independently review their compliance with law and ministerial direction.[130] With respect to the RCMP, the Auditor General concluded that the Commission for Public Complaints Against the RCMP does not have

---

[127] Office of the Auditor General, *March 2004 Report* — Chapter 3: 'National Security in Canada The 2001 Anti-Terrorism Initiative'.

[128] Now the Canada Revenue Agency.

[129] Report of the Auditor General of Canada, November 2003, para. 10.139.

[130] *Ibid*, Para. 10.154.

the same level of access to RCMP information as the Inspector General and SIRC have to CSIS information.[131]

The Auditor General also noted that just as the mandates of review agencies vary, so does reporting and disclosure of findings to Parliament.

The Auditor General recommended that:

> The government should assess the level of review in reporting to Parliament for security and intelligence agencies to ensure that agencies exercising intrusive powers are subject to levels of external review and disclosure proportionate to the level of intrusion.[132]

In response to this recommendation for comprehensive review of this situation, the Privy Council noted the various agencies and departments in the security and intelligence community operate under quite different mandates and legislation.

## G. THE INFORMATION AND PRIVACY COMMISSIONERS

Accountability to the public is also achieved through various mechanisms of public reports from national security agencies, public inquiries, parliamentary committees, and external review bodies. In the area of national security, there are usually limits on the public's right to know. The legal definitions of information that may be disclosed, or may not be disclosed, in terms of security considerations, are thus of considerable significance for accountability. As well, citizens have a legitimate interest in what kind of personal information the state retains about them, and what use might be made of such information, especially in the area of national security, where individual rights are always being weighed against public safety. In 1985, Parliament passed the *Access to Information Act*[133] and the *Privacy Act*[134], and established the offices of the

---

[131] *Ibid*, Para. 10.146.

[132] *Ibid*, Para. 10.162.

[133] R.S.C. 1985, c. A-1.

[134] R.S.C. 1985, c. P-21.

Information Commissioner and the Privacy Commissioner.

The purpose of the *Access to Information Act* is "to extend the present laws of Canada to provide a right of access to information in records under the control of a government institution in accordance with the principles that government information should be available to the public, that necessary exceptions to the right of access should be limited and specific and that decisions on the disclosure of government information should be reviewed independently of government."[135] In other words, members of the public can file requests with government institutions for access to documents and information in the hands of these institutions. The public's right of access is subject to certain limits. The Information Commissioner, an independent ombudsman appointed by Parliament, investigates complaints from people who believe they have been denied rights under the *Access to Information Act*. In this capacity, the Information Commissioner is the avenue for appeal for Canadians denied access to information on national security they have requested. The *Access to Information Act* provides that "the head of a government institution may refuse to disclose any record requested under this Act that contains information the disclosure of which could reasonably be expected to be injurious to the conduct of international affairs, the defence of Canada or any state allied or associated with Canada or the detection, prevention or suppression of subversive or hostile activities."[136] Section 16 widens this category to include information relating to criminal investigations, law enforcement, and "activities suspected of constituting threats to the security of Canada within the meaning of the *CSIS Act*." To satisfy the terms, the government must establish that harm will result from the specific disclosure. In the case of disagreement, the Information Commissioner will attempt to negotiate a settlement between the complainant and the government institution, but may also represent a complainant before a Federal Court review in the event that no agreement has been reached.

The *Access to Information Act*, in the hands of investigative journalists, academics, and private citizens, has provided a tool for disclosure of information regarding various aspects of national

---

[135] S. 2(1).

[136] S. 15(1).

security policy and performance. Indeed, much information in reports of review bodies like SIRC and the IG has only been disclosed through *Access* requests. At the same time, there have been no instances cited by government in which information injurious to Canadian national security has been released as a result of the Access law. However, some government departments and agencies have been critical of the perceived negative effect of the law on the operations of government.[137] The 2001 *Anti-terrorism Act* introduced several new limitations on access to national security information, as well as a new *Security of Information Act*[138] that replaces the *Official Secrets Act*. Some have argued on the other hand that reasonable access to information consistent with national security is a primary constituent of any accountability system, and that the Information Commissioner in his or her capacity as an ombudsman or advocate on behalf of citizens seeking access is thus an important element in an effective accountability mechanism.[139]

The office of the Privacy Commissioner is established under the *Privacy Act*, the purpose of which is to "extend the present laws of Canada that protect the privacy of individuals with respect to personal information about themselves held by a government institution and that provide individuals with a right of access to that information."[140] The right of access is potentially limited by a number of restrictions concerning national security and law enforcement that parallel the restrictions in the *Access to Information Act*. The Privacy Commissioner investigates complaints of citizens concerning access to their personal information, but more generally acts as an advocate for the privacy rights of Canadians, conducting and publishing research on privacy practices of government, and "promoting awareness and understanding of privacy issues by the Canadian public". In this latter capacity, a former Privacy Commissioner in his 2001-2002 Annual Report criticized the privacy implications of the post-9/11 anti-terrorist

---

[137] Donald J. Savoie, *Breaking the Bargain: Public Servants, Ministers, and Parliament* (Toronto: University of Toronto Press 2004) pp. 49-52.

[138] R.S.C. 1985, c. O-5.

[139] Reg Whitaker, 'Access to information and research on security and intelligence: the Canadian situation', in Peter Hanks and John D. McCamus, eds., *National Security: Surveillance and Accountability in a Democratic Society* (Cowansville, Quebec: Les Editions Yvon Blais, 1989) pp. 183-196.

[140] S. 2.

measures of the Government of Canada. The 2001-2002 report highlights a potential advocacy role for the Privacy Commissioner in promoting privacy rights in the national security area. SIRC and the CSE Commissioner have their own role to play in protecting privacy rights of citizens before the organizations they review, as well as handling complaints in this area.

The Information Commissioner has recently argued in favour of merging his office with that of the Privacy Commissioner, along the lines of most provincial information and privacy bodies.[141] The government has to date not implemented this suggestion, but if a merger were to be effected in the future, the implications for national security accountability are unclear.

## H. PARLIAMENTARY REVIEW

As previously noted, a significant departure from the McDonald Commission recommendations in the *CSIS Act* was the disinclination of the government to establish a committee of Parliament as a central player in the review process. SIRC, with a composition intended to broadly reflect the parties in Parliament, was instead seen as a sort of surrogate, or replacement, for an active parliamentary committee. Peter Russell, who had been the Research Director for the McDonald Commission, was critical of the government's omission of a permanent joint parliamentary committee and doubted that SIRC could effectively replace such a committee.[142] The reason for this decision is not clear, although there may have been a concern that partisan politics were not conducive to developing effective accountability in national security matters.[143] At the same time, one academic observer has noted that independent review is not democratic doctrine, but

---

[141] Office of the Information Commissioner of Canada, Position Paper: 'Oversight Models under the Federal Access and Privacy Acts: Single Commissioner vs. Dual-Commissioners' (Ottawa 24 Oct. 2003).

[142] Peter Russell, "The proposed charter for a civilian intelligence agency: an appraisal", *Canadian Public Policy* 9:3 (1983) p. 337.

[143] Wesley Wark, 'Terrorism: It's time to grow up', *The Globe & Mail*, April 1 2004, p. A17: "Opposition politicians don't yet get a fundamental requirement of public debate over national security issues, especially ones that touch on intelligence matters. That requirement is for bipartisanship. National security matters are too important to be treated as political cannon fodder, an understanding rooted in both the British parliament's structure for intelligence-community oversight and in the U.S. congressional-committee system. That lesson will have to sink home fast, as the Paul Martin government has promised the creation of Canada's first permanent parliamentary committee to study national security issues."

"management doctrine" based on a formula of checks and balances between appointed officials, that threatens to be undemocratic unless "closely directed and scrutinized by elected officials".[144]

It is interesting that in the one specific role for Parliament established in the *CSIS Act*, the mandated five-year review of the Act, the parliamentarians seemed to proceed in a manner that was free of partisan considerations. The first five year review report was unanimous, and bore no evidence of partisan disagreement.[145] The official response to this report was mixed. A few specific suggestions were adopted, but most recommendations were not. The government was not especially co-operative with the committee during its deliberations, especially with regard to access to information issues. Since the committee members lacked security clearance, their efforts to adduce information in protected areas left them more or less in the same situation as private citizens using the *Access to Information Act*. Even SIRC was unable to be fully co-operative with the committee, given the constraints imposed upon it with regard to disclosure.[146]

Following the release of the report, the chair of the five-year review committee followed up by constituting a permanent Subcommittee on National Security, drawing on the same membership and the new base of expertise that had been built up.[147] The subcommittee chose not to seek security clearance for its members, believing that that secret proceedings would compromise their ability to fulfill a public role. It may be that such a subcommittee could work in a complementary fashion with SIRC, which did have access to secret information. This could be a possible way to reconcile the McDonald idea with the *CSIS Act*, but it did not work out in practice.

---

[144] Sharon L. Sutherland, 'Independent review and political accountability: should democracy be left on autopilot?', *Optimum* 24:2 (Autumn 1993) p. 24.

[145] Canada, House of Commons, Report of the Special Committee on the Review of the *CSIS Act* and the Security Offences Act, *In Flux but not in Crisis* (Ottawa: September 1990).

[146] See the account of the committee's difficulties by its research director: Stuart Farson, 'The Noble Lie Revisited: Parliament's Five-Year Review of the *CSIS Act*: Instrument of change or weak link in the chain of accountability?' in Philip C. Stenning, ed., *Accountability for Criminal Justice: Selected Essays* (Toronto: University of Toronto Press, 1995) pp. 185-212.

[147] For an overview, see Stuart Farson, 'Parliament and its servants: their role in scrutinizing Canadian intelligence', *Intelligence & National Security* 25:2 (Summer 2000), pp. 225-258.

The Senate has not been silent in this area. In the late 1980s, a Special Committee of the Senate on Terrorism and the Public Safety reported a series of policy recommendations.[148] More recently, the Senate Committee on National Security and Defence has issued a number of reports on such matters as airport and seaport safety and national emergency preparedness that have been taken very seriously by the appropriate government departments.[149] It is no reflection on the work of senators, however, to observe that the members of the upper chamber are appointed and not elected. Thus the question of the role of the Commons has remained central.

In 2004, the Government published a consultation paper on a national security committee of parliamentarians, for the purpose of encouraging a debate on the establishment of a parliamentary mechanism with a "strategic mandate" to review the larger picture regarding the government's conduct of national security. The members might be Privy Councillors, like the members of SIRC, and thus have access to secret information. Such a committee would not be seen as replacing the existing external review bodies, but perhaps as working with them in complementary fashion.[150] This proposal was tabled prior to the dissolution of the 37th Parliament and the 2004 general election. The Committee has not, however, been formally established, although an Interim Committee on National Security will be publishing recommendations shortly on the composition and mandate of the proposed Committee. Whatever specific form this idea eventually takes, it offers the possibility that the final link in the accountability system post-McDonald may be filled in.

---

[148] Canada, *Report of the Senate Special Committee on Terrorism and the Public Safety* (June 1987).

[149] Most recent in a series of reports: Standing Senate Committee on National Security and Defence, *National Emergencies: Canada's Fragile Front Lines: An Upgrade Strategy* v. 1 (March 2004).

[150] 'A National Security Committee of Parliamentarians', Consultation Paper to help inform the creation of a committee of parliamentarians to review national security (Ottawa 2004).